Mayank V. Bendarkar, Ameya Behere, Simon Briceno, Dimitri N. Mavris. "A Bayesian Safety Assessment Methodology for Novel Aircraft Architectures and Technologies using Continuous FHA", AIAA Aviation 2019 Forum (AIAA 2019-3123) https://doi.org/10.2514/6.2019-3123
https://arc.aiaa.org/doi/10.2514/6.2019-3123

A Bayesian Safety Assessment Methodology for Novel Aircraft Architectures and Technologies using Continuous FHA

Mayank V. Bendarkar*, Ameya Behere †, Simon Briceno ‡, and Dimitri N. Mavris§
Aerospace Systems Design Laboratory, Georgia Institute of Technology, Atlanta, Georgia, 30332

Novel architectures and technologies carry with them an uncertainty related to their reliability and associated safety risk. Existing safety assessment methods involve determining the severity of discrete functional failure and the corresponding probability. However, with the advent of novel aircraft architectural and operational concepts, traditional methods of establishing severity and probabilities failures are found lacking due to the scarcity of available data. The current work proposes a safety assessment method that uses architecture-specific performance models along with continuous functional hazard assessments to inform hazard severity. The probability of failures is determined using a Bayesian framework that does not falter when data is scarce. Taken together, it is expected that this new proposed methodology will enable a more accurate safety assessment of novel aircraft architectures and technologies. A safety assessment of an electric propulsion system powered by a fuel cell is conducted using the proposed methodology to serve as a proof of concept.

Nomenclature

C-FHA	=	Continuous Functional Hazard Assessment
λ	=	Failure rate (per flight hour)
$\bar{y}$	=	Available failure data
a	=	Compliance action (decision)
X	=	True value of compliance finding (unknown)
δ	=	Decision rule
$L(X, a)$	=	Loss function

I. Introduction

General Aviation (GA) aircraft account for more than 90% of the registered civil aircraft fleet in the US [1]. This segment is likely to be at the forefront of a paradigm change in aviation where introduction of novel concepts such as Urban Air Mobility (UAM), architectures like $e-$VTOL, and technologies like hybrid electric propulsion are expected to make aircraft more efficient and reduce their environmental footprint. However, these architectures carry with them an uncertainty related to their reliability and the safety risk they pose. To ensure the continued safety of the GA fleet and operations in this rapidly evolving new paradigm, the Federal Aviation Administration (FAA) implemented a new set of performance-based certification rules for Normal Category Aircraft in Title 14 of the Code of Federal Regulations (CFR), Part 23, Amendment 64 [2]. Compliance with these rules can now be shown using means of compliance information given in approved consensus standards like those developed by ASTM Committee F44 on General Aviation Aircraft [3, 4]. While a parallel effort looks at simplifying the documentation process involved in certification using a Model-Based System Engineering (MBSE) approach [5], of particular interest in this paper is FAR §23.2510 which requires that all equipment, systems, and installations have [2]

> "a logical and acceptable inverse relationship between the average probability and the severity of failure conditions."

It is paramount for aircraft designers to have the capability to quantify safety risk earlier in the design phases to help mitigate avoidable surprises once the aircraft is already built. Safety risk is generally quantified as a combination of two

*Senior Graduate Researcher, Daniel Guggenheim School of Aerospace Engineering, AIAA Student Member
†Senior Graduate Researcher, Daniel Guggenheim School of Aerospace Engineering, AIAA Student Member
‡Senior Research Engineer, Daniel Guggenheim School of Aerospace Engineering, AIAA Senior Member
§S.P. Langley NIA Distinguished Regents Professor, Daniel Guggenheim School of Aerospace Engineering, AIAA Fellow

Assessment Level	Failure Condition Classification				
	Negligible	Minor	Major	Hazardous	Catastrophic
I	No Probability Requirement	$<10^{-3}$	$<10^{-4}$	$<10^{-5}$	$<10^{-6}$
II		$<10^{-3}$	$<10^{-5}$	$<10^{-6}$	$<10^{-7}$
III		$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-8}$
IV		$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-9}$

Table 1 Quantitative Allowable Failure Rate for Different Failure Conditions [8] *

entities – the probability of a failure or an unsafe event, and the severity associated with it [6]. The probability of a failure or an unsafe event is the frequency with which it can be expected to occur, and is generally quantified using historical data [7]. The severity of failure denotes the impact of failure, and is generally classified into five categories depending on whether such failure puts life or property in harms way. Table 1 shows the failure classification conditions and the corresponding allowable failure rates for GA aircraft [6, 8]. Generally speaking, the severity is defined as – (i) *Catastrophic* when there is a chance of multiple fatalities and/or total loss of aircraft (ii) *Hazardous* when it may result in serious injuries or some loss of life (iii) *Major* when there is a significant reduction in safety or functional capability of the aircraft with expected safe flight, and (iv) *Minor* when there may be little loss of safety margins but no expected injuries or damage [9].

The intent of safety assessments is to ensure that any system under consideration poses no worse than an acceptable level of risk. SAE ARP4754A and SAE ARP4761 act as accepted and well established guides for performing safety assessments [6, 10]. In the early design phase, ARP4761 suggests conducting a Functional Hazard Assessment (FHA), which is defined as [6]:

> "A systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity."

The aircraft and system level FHA aims at identifying the hazards associated with functional failure at the corresponding levels while including considerations for environmental conditions and flight phase. This usually results in two types of functional requirements – (i) *Availability* (e.g. the loss of function), and (ii) *Integrity* (e.g. Malfunction) [11]. The allowable probability of functional failure is determined by Table 1 once the corresponding hazard severity is established. Once FHAs are completed, airplane and system functional designs or architectures are proposed to meet the generated safety requirements. The verification of functional designs take the form of a numerical analysis [11]. There are two types of analysis methods prescribed to complete this – (i) Top-Down methods that include dependency diagrams, Fault Tree Analysis (FTA) among others, and (ii) Bottom-Up methods that include the Failure Mode Effects and Criticality Analysis (FMECA). Figure 1 shows an overview of the relationship between FHA and FTA in conceptual and preliminary design. FTA, which forms an important component of Preliminary System Safety Assessment (PSSA) (see Fig. 1), is verified using FMECA by postulating failure mechanisms at the component level, and with the addition of failure probability data should give a close correlation to the FTA conducted [9]. As the design progresses from the conceptual phase to the preliminary phase, functional safety assessments are followed by physical assessments that focus on physical layout and validate the redundancy and independence assumptions made. Finally, operational safety requirements are generated out of unusual scenarios, with unsatisfactory results being fed back into the design process [11].

It is important to note that the current paradigm seeks to identify hazards early in the design process and percolate corresponding qualitative or quantitative safety requirements downstream. Washington et al.[12] summarize the outcome of the system safety assessment process as four related sets F, C, Λ and O where:

1) F is the set of n identified failure conditions $f_1 \; - \; f_n$
2) C is the set of severities c_i assigned to each failure condition f_i
3) Λ is the set of probabilities λ_i of each failure condition f_i, and
4) O is the set of failure probability objective o_i associated with f_i and its severity c_i as given by table 1

The current safety assessment paradigm is not without its limitations. In the conceptual and preliminary design phase, the existing approach of safety assessment seeks to limit the risk posed by any failure condition f_i by ensuring that the probability of said failure λ_i is less than its probability objective o_i as determined by Table 1 using severity

*Assessment levels for General Aviation (GA) aircraft are defined based on the number of passengers[13]

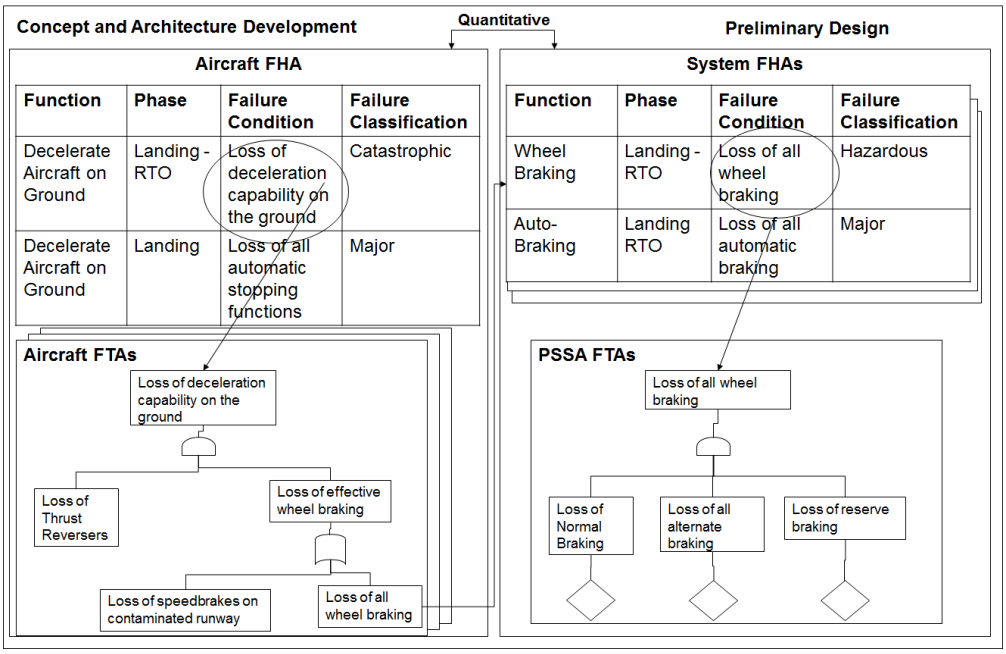


Fig. 1 Overview of safety assessment methods in conceptual and preliminary design: Relationship between FHAs and FTAs [6]

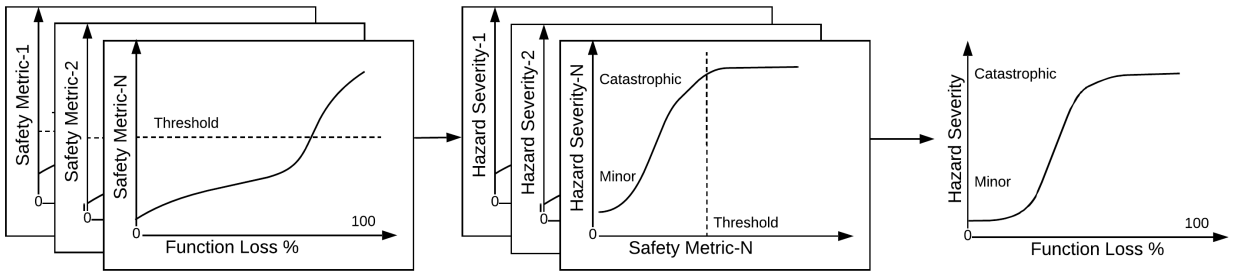
c_i. Traditional FHA is a tabular approach in which discrete functional failures are assigned a discrete hazard severity as shown in Table 1. This makes the process slow and time consuming, requiring an analyst to analyse every unique architecture configuration manually, thus limiting the scope for design space exploration in the early design phase. At the same time, novel architectures and technologies may not have discrete functional failures, and their consequences may not be well understood. Qualifying a functional failure discretely merely as *loss of function* or *malfunction* may not provide the full picture in terms severity of said failures. One solution in the traditional approach is to assign a conservative estimate to the severity posed, resulting in incorrect unit level probability requirements (o_i) in the early design process. As Armstrong states in his PhD thesis [14]:

> "Assumptions regarding the relationship between function loss and hazard severity employed during traditional Functional Hazard Assessment bias architecture design and lead to inaccurate estimation of unit level requirements."

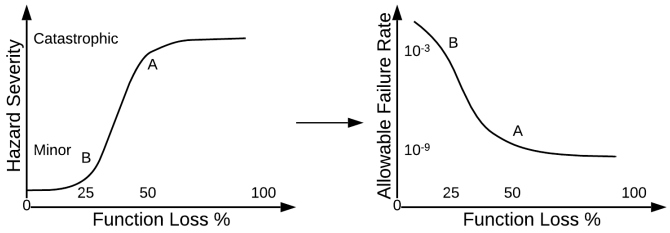
Consider for instance a Distributed Electric Propulsion (DEP) concept. Instead of the traditional scenarios (loss of thrust/ one engine out), the DEP is likely to have a spectrum of thrust degradation scenarios (0% to 100% thrust loss). Since there is little historical precedent to these architectures and scenarios, the current approaches fall short in qualifying the severity of functional degradation and can potentially result in incorrect functional hazard severity allocation. At the same time, ARP 4761 cannot comprehensively address uncertainty in input data and models [12]. Uncertainty is generally classified into two categories [15]:

- Epistemic Uncertainty (Greek *'episteme'*: knowledge) is also called knowledge-based uncertainty that results from incomplete knowledge or understanding about fundamental phenomenon. This uncertainty is significant in situations where not enough evidence or data is available.
- Aleatory Uncertainty (Greek *'alea'*: game of chance) is the second type of uncertainty and relates to the inherent randomness or stochasticity of a system that is not reducible.

The common method used to determine probability of an event (component failure for instance) in ARP4761[6] is using what is called a *'Frequentist approach'* by modern statisticians. The *Frequentist approach* can only take aleatory uncertainties into account through data that is available [15]. To mitigate this downside, ARP4761 suggests in making conservative assumptions to deal with its limitations and manage uncertainty better [6, 12]. However, with novel architectures and concepts of operation, data available are insufficient and epistemic uncertainty is large, thus rendering existing (Frequentist) probability models unsuitable [12, 16]. It is on this premise that the current work is motivated. The intent of this paper is to supplement the current safety assessment techniques (See [6, 9, 11, 17–19]) with a methodology that can address the shortcomings mentioned above.



(a) Hazard severity with continuous functional degradation



(b) Allowable failure rate for the given severity curve

Fig. 2 Notional plot of the C-FHA process

The rest of this paper focuses on describing the proposed approach (Sec II), showcasing the proposed approach using a case study on a fuel cell propulsion system (Sec III), followed by conclusions (Sec IV).

II. The Proposed Bayesian Safety Assessment Methodology

The proposed approach seeks to supplement existing methods by addressing some of the limitations mentioned in Sec. I. In particular, the new approach differs from the traditional methods in both determining probability of failures as well as establishing the severity associated with them. The approach also seeks to enable design space exploration to be conducted in early design phases while including system safety considerations. The new approach is shown in Fig. 4, the important components of which are a Continuous Functional Hazard Assessment (C-FHA) and a Bayesian Probability Assessment. These are discussed in greater detail below:

A. Severity Assessment: Continuous Functional Hazard Assessment

The functional decomposition of a novel system architecture or technology is likely to remain similar to a conventional system even if the implementation varies drastically between the two. For example, an airborne system is likely to have a function *Generate Lift* to stay airborne, or *Provide Thrust* to translate irrespective of whether it is a conventional tube and wing aircraft or a distributed electric VTOL concept. Traditional Functional Hazard Assessment (FHA) utilizes this knowledge to keep implementation and behavioral spaces independent while characterizing hazards [20]. Traditional FHA considers discrete off-nominal scenarios, for e.g. – 1)loss of function, 2) excess function, and 3)incorrect operation of function. However, as explained in Sec. I for novel concepts and architectures, it is important to differentiate off-nominal scenarios that can result in continuous functional degradation.

Armstrong made a case for Continuous FHA (C-FHA) that assigns a continuous hazard severity that depends on continuous functional degradation [14]. C-FHA extends the traditional FHA and system safety analysis methods to consider the magnitude of function loss when assessing an architecture or a concept and is notionally shown in Fig. 2. As a first step, the analyst defines safety critical metrics of interest under functional degradation scenarios for different flight phases. For example, when the aircraft function of interest is *'Provide Thrust'*, metrics like required Take-off Field Length (TOFL) or required climb gradient can be computed using the information available in early design phases under thrust degradation scenarios. With additional knowledge about the aircraft concept like a calibrated 6-DoF model, metrics like abnormal attitude, airspeed, angular rates, asymmetric forces, or flight trajectory – that correlate to loss of control situations can be computed for a thrust degradation scenario to paint an accurate picture of the aircraft's

departure from safe operation. Energy based metrics for safety analysis like those described by Puranik [21, 22] can also be considered for this purpose. Second, these metrics are calculated based on available performance models of the appropriate fidelity under functional degradation scenarios. The results of such functional degradation scenarios for different flight phases can then be combined and translated into hazard severity curves for the given scenario or phase of flight by decision makers leading to the creation of C-FHA curves. Generating continuous hazard severity curves instead of discrete values suggested by Table 1 can allow decision makers to account for uncertainty in the models utilized to compute safety metrics of interest [14].

Figure 2 provides a notional plot showing how hazard severity can be obtained as a function of continuous functional degradation while also showing how the generated hazard severity-function loss curve can be translated into an allowable failure rate-function loss curve using Table 1. The effect of functional degradation is computed on various safety metrics using available models for a particular flight phase. Decision makers can then utilize this knowledge to define hazard severity curves for every case, which can then be combined into one hazard severity curve for the function under consideration for the flight phase of interest. This final hazard severity - function loss curve now provides a physics backed relationship between the two, as opposed to a heuristic and case by case approach provided by traditional FHA. The continuous hazard severity results in safety requirements that are allocated to the system level function in terms of allowable failure rate (see Table 1). Failures in subsystems or components are likely to result in degradation in the system's capability to perform certain functions. A model that can determine the effect of component failure to the system level functions can now be utilized to generate component level reliability requirements based on generated hazard severity-functional degradation relationship. As shown in Fig. 2, if the failure of component A or B results in a 50% and 25% functional degradation at the system level, the requirement for allowable failure rates for these components can be generated using the same plot. In reality, such a model will need to be combined with a reliability block diagram (RBD) to determine system reliability requirements as a function of functional degradation scenarios.

The C-FHA method described above can allow engineers to (i) Determine a physics backed relation between functional degradation scenarios and corresponding hazard severity levels using performance and modeling tools available in the corresponding design phase, and (ii) Allocate system level failure rate requirements accurately to the component level. Since C-FHA utilizes knowledge of the system in terms of performance models available at the time of conducting this analysis, this method can be utilized to model novel aircraft concepts, architectures, and technologies by utilizing information available in early design phases. As the design matures, C-FHA allows engineers to update the failure rate requirements generated by utilizing higher fidelity models to determine the effects of functional degradation on system safety metrics. Additionally, decision makers only need to interact with C-FHA to determine the appropriate hazard severity curves to be used. All other aspects of this method can be easily automated to allow a design space exploration exercise while considering component reliability requirements.

B. Bayesian Probability Assessment

A Bayesian approach of estimating probability allows for the treatment of both epistemic and aleatory uncertainty even when available data is limited. Instead of only using data, a Bayesian approach relies on using information - which includes data, models, and other available information like subject matter expert (SME) knowledge [16]. Furthermore, a Bayesian inference model can be continuously updated as additional information becomes available. Bayesian inference techniques for safety and reliability assessment have been applied to numerous problems in literature [23–26] and are considered mature and mathematically sound for the purpose. The utility of this approach can be attested to when one considers that numerous industries consider these techniques standard [27–30].

Under the Bayesian framework, uncertainty in the failure rate (λ) conditioned over available failure data ($\bar{y}$) is given by the conditional distribution $p(\lambda|\bar{y})$ as given by Eq. 1

$$p(\lambda|\bar{y}) = \frac{p(\bar{y}|\lambda)p(\lambda)}{p(\bar{y})} \tag{1}$$

Equation 1 gives the Bayesian posterior distribution $p(\lambda|\bar{y})$ based on the likelihood of observing the data that was observed $p(\bar{y}|\lambda)$, and the analyst's prior belief $p(\lambda)$ normalized over all realizations of the data $p(\bar{y})$. Note that Eq. 1 is simply a statement of Bayes' theorem applied to multiple independent identically distributed observations $\bar{y}$.

1. Likelihood Distribution

The likelihood $p(\bar{y}|\lambda)$ is a function of λ that seeks to determine the likelihood of the observed data $\bar{y}$ given λ. It is a statistical model used to represent the aleatory uncertainty associated with the data and its underlying physical

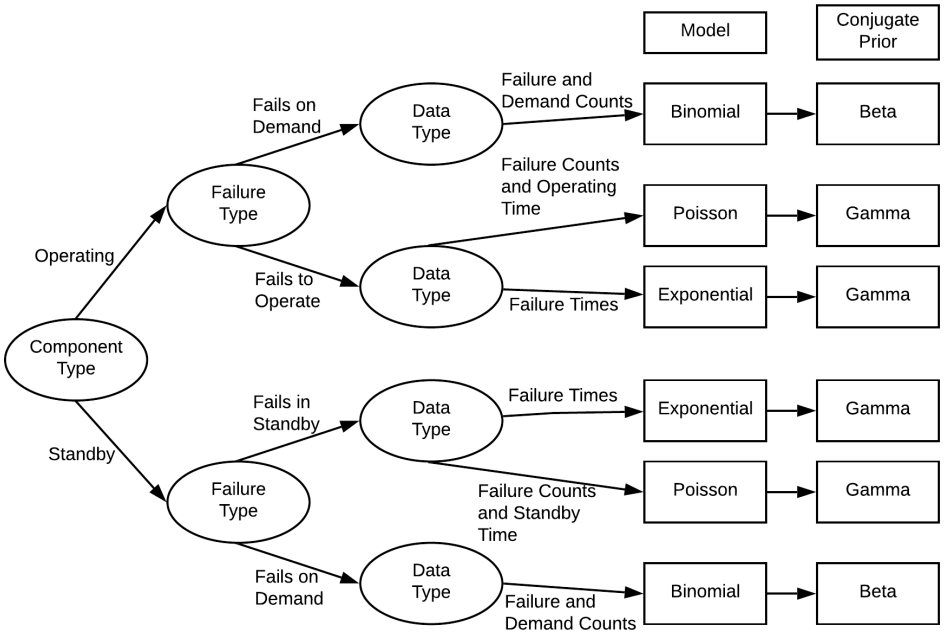


Fig. 3 Guidelines for selecting the Likelihood and Conjugate Prior Distributions [16]

phenomenon [12].

The three most common distributions used to model aleatory uncertainty are the Binomial, Poisson, and Exponential distributions [16]. Figure 3 provides a guideline for the different types of likelihoods that can be used to model failure phenomenon related to aerospace operations. As can be seen in Fig. 3, a Binomial distribution is generally used to model failures on demand, a Poisson distribution is used when there are failures in time or initiating event, and an Exponential distribution is used when the time to failure or time to recover are being modeled.

2. Prior Distribution

The prior distribution $p(\lambda)$ captures information that is denoted by the analyst's subjective state of belief regarding the failure rate. Since this distribution is based on the analyst's knowledge about the component or event, it captures the epistemic uncertainty associated with estimating the failure rate (λ) [12]. Informative and non-informative priors are two broad categories of prior distributions. The non-informative priors seek to minimize the information bias within a prior and let the data dominate the posterior. Informative priors contain information that can influence the posterior and can be generated by combining the analyst's own knowledge with SME opinion on the unknown parameter (λ)[16]. Additionally, conjugate priors can be used with certain likelihood functions to ensure that the posterior follows the same family of distributions. This can allow an analyst to have analytical solutions for the posterior and simplify calculations. In cases of non-conjugate priors, numerical methods like Markov Chain Monte Carlo can be used to determine the posterior.

If an event has a probability of zero set by the prior, no amount of data observed otherwise can change the posterior. It is for this reason that prior choices need to be made carefully by the analyst. Additionally, in the absence of data, the prior distribution becomes the posterior! Figure 3 provides suggestions on appropriate prior distributions that can be used for certain cases pertinent to aerospace applications. The reader is directed to the work of Dezfuli et al. [16], which provides comprehensive guidance on selecting the appropriate distributions to model the priors by considering opinion of SMEs and available data for component failures in other domain applications among other cases.

3. Posterior Distribution

The likelihood function multiplied by the prior distribution gives a joint distribution of the data and parameter λ. The normalizing constant in the denominator $p(\bar{y})$ can be obtained by integrating λ out of this joint distribution to give

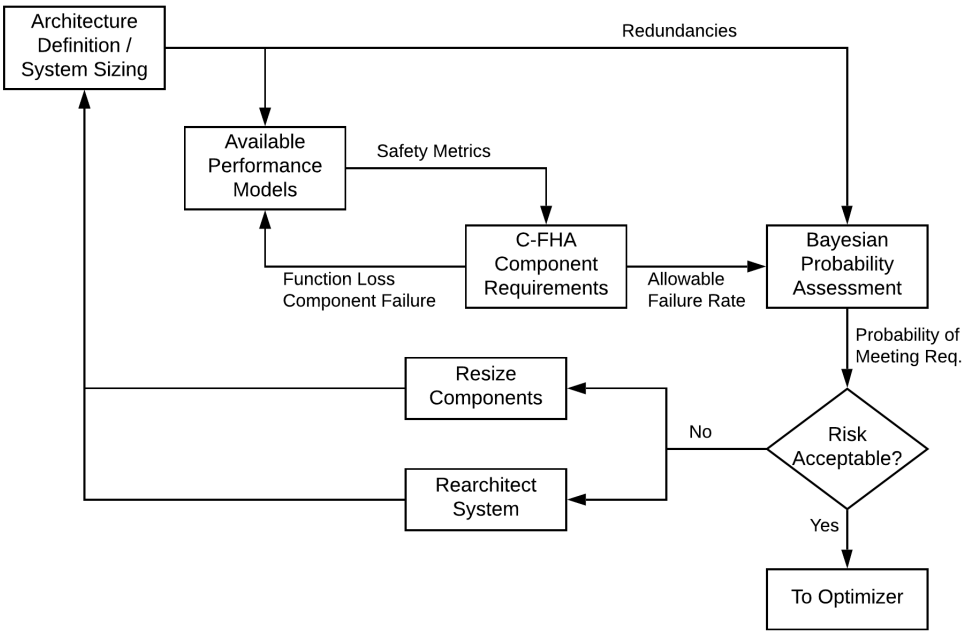


Fig. 4 Proposed methodology for safety assessment integrated with design of novel architectures

the posterior distribution given by Eq. 2.

$$p(\lambda|\bar{y}) = \frac{p(\bar{y}|\lambda)p(\lambda)}{\int_\lambda p(\bar{y}|\lambda)p(\lambda)} \tag{2}$$

This posterior distribution provides an updated state of knowledge of the failure rate taking into account the analyst's subjective state of belief and available data. Certain heritage data can also be utilized by eliciting its applicability from subject matter experts (SMEs), and averaging the posterior distributions according to the applicability of the data [16]. If there are no data available, the posterior is the same as the prior. The prior influence on the posterior reduces as more and more data become available, resulting in the posterior moving closer towards the Frequentist estimate. A Bayesian approach has numerous benefits over the traditional Frequentist approach (in addition to treating uncertainty more comprehensively) for application to safety assessment of novel aircraft concepts.

- The Bayesian posterior can be continuously updated as more data become available. This is done by treating the existing posterior as a prior for the new data and generating a new posterior.
- A 95% posterior credible interval for λ has a 95% probability of the true value of λ lying within it [31], unlike the more complicated interpretation of Frequentist confidence intervals.[†]

C. Integrated Risk and Compliance Assessment: A Bayesian Decision Framework

Figure 4 provides an overview of the overall risk assessment method proposed here. It is assumed that the configuration has been sized and adequate performance models are available to determine the level of functional degradation if certain components fail. The proposed method begins with the C-FHA method described in Sec. II.A. System level safety-critical functions are defined and the effect of a continuous degradation in said functions on safety critical metrics of interest is determined to allow decision makers to allocate hazard severity. At the same time, effect of subsystem or component level failures in terms of function loss is computed using the performance models available. Next, combining the severity allocated to functional degradation, the effect of component failure in terms of system function-loss, and the allowable failure rate determined from Table 1, probability requirements are allocated to the subsystems or components of interest. Finally, the probabilities of component failures can be estimated using a Bayesian approach as explained in Sec. II.B. The combination of C-FHA to yield component level reliability requirements and Bayesian probability estimation to yield posterior distributions of component failure rates λ allows the analyst to compute

[†]A 95% Frequentist confidence interval states that if a sample of failure data were collected a large number of times, 95% of the generated confidence intervals will contain the true λ [31]; an interpretation that is not very useful in the current application.

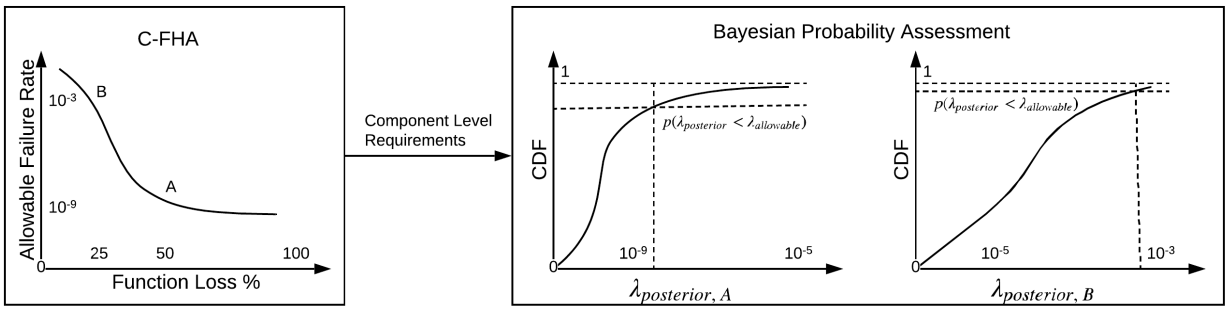


Fig. 5 Integrated Risk Assessment - Probability of meeting component reliability requirements

the probability with which reliability requirements can be met. This is shown notionally in Fig. 5. The probability that component B can meet the reliability requirement is given by the dashed line showing $p(\lambda_{posterior} < \lambda_{allowable})$ on the CDF of the posterior failure rate of B.

Decision makers now need to make a decision on whether the corresponding probability of meeting requirements is good enough to consider component B (See Fig. 5) within the architecture under consideration, compliant with the safety requirements. In a Bayesian decision theoretic setup, such a compliance decision regarding component B is considered an *action* $a \in A$ ($A = \{compliant, non-compliant\}$). The *action* to be taken as a function of observation or data is considered a *decision rule* (δ). Finally, a loss function $L(X, a)$ represents the penalty to be paid if the analyst chooses *action* a, under available information $p(\lambda_{posterior} < \lambda_{allowable})$, when the true value of the compliance finding is $X = \{compliant\}$ or $X = \{non-compliant\}$. The Bayesian expected loss is the expectation of the loss function with respect to the posterior failure rate computed, and is given by:

$$\rho(a, p) = \int_{\lambda} L(X, a) p(\lambda|\bar{y}) \delta\lambda \tag{3}$$

An action a^* that minimizes the expected loss given by Eq. 3 should be the action taken by the analyst, and is called *Bayes action*. It is important to note that this Bayes decision framework provides the analyst with a mathematically defensible method of making compliance finding with safety requirements while accounting for epistemic and aleatory uncertainty. This proposed framework can thus address some of the limitations of the traditional safety assessment process for novel system concepts, architectures, and technologies.

The next section focuses on demonstrating the methodology discussed in Sec. II on a notional fuel cell power system for GA aircraft. In this paper, a simple loss function in terms of a loss matrix will be considered for demonstration (see Sec. III.C).

III. Case Study: A Fuel Cell Power System

A fuel cell is a device that uses electro-chemical reactions to convert chemical energy into electricity. The reactants are the fuel – usually Hydrogen gas, and an oxidizing agent. These reactants flow in at the anode and cathode respectively where they react with the electrolyte and produce water and electricity. A notional fuel cell is depicted in Fig. 6. For practical applications, a number of fuel cells are connected to form a fuel cell stack. With the help of an electric motor powered propeller, such a system can be adapted for aircraft propulsion.

Although the reactants and the end products are similar to a combustion reaction, there are a few key differences. The energy released in the reaction is in the form of electric current rather than heat. The temperatures at which the oxidation occurs is also much lower than a typical combustion temperature. The reaction mechanism itself is also quite different. A typical mechanism for an acidic fuel cell follows these steps.

1) Hydrogen gas enters the anode side of the cell. This gas may be either stored in fuel tanks directly or produced from other compounds such as methanol in a reformer. At the anode, the gas dissociates into protons and electrons. The protons enter the acidic electrolyte and the electrons are left at the anode

$$2H_2 \longrightarrow 4H^+ + 4e^- \tag{4}$$

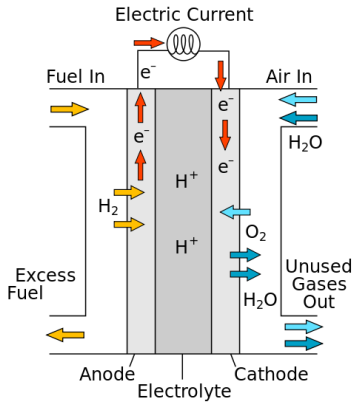


Fig. 6 Schematic of a notional proton conducting fuel cell [32]

2) The oxidizing agent flows at the cathode where it reacts with the protons to form water.

$$O_2 + 4H^+ + 4e^- \longrightarrow 2H_2O \tag{5}$$

3) The protons flow through the proton conducting electrolyte. An external circuit is created which links the two electrodes. This enables the electrons to flow from the anode to the cathode, thus constituting an electric current.

When used for transport applications, the type of fuel cell used is generally dominated by its power to weight ratio. As a result, the Proton Exchange Membrane (PEM) type of fuel cell a common choice for such applications due to its low weight and volume. The mechanism of this cell is similar to that of an acidic fuel cell as the electrolyte promotes the movement of protons. In order to optimize the performance, a number of design features are often incorporated to increase the efficiency and power output [33].

- To speed up the reaction, platinum is used as a catalyst. The construction involves careful placement of platinum particles on graphite electrodes. Further, since the reaction site has to host the reactant gases, the electrolyte is built as a porous membrane.
- For increased power output, the reactants gases are fed in at high pressure. If ambient air is being used as an oxidizing agent, then the partial pressure of oxygen has to be raised accordingly.
- As with many other chemical reactions, the rate of the reaction is highly dependent on the temperature, with a higher rate of reaction at higher temperatures. There is an upper limit to the benefit of raising the temperature as beyond a certain point, there is significant degradation to the intricate construction of the cell itself.

Although fuel cells propulsion systems are well understood for automobiles, they are still an upcoming concept for aviation. The operating envelope for an aircraft contains highly variable ambient conditions than an automobile might experience. There is a need to study the performance of fuel cell propulsion systems at these extreme conditions to assess their implications on aircraft safety. In this case study, a fuel cell propulsion system is modeled from first principles. To maintain efficiency and sufficient power outputs, several external components are used to condition the ambient airflow before it reaches the cathode. A generic model of a fuel cell based propulsion system adapted for aviation use is shown in Fig. 7. The components, in the order experienced by the airflow are a compressor, heat exchanger and a humidifier.

- The compressor is needed to raise the partial pressure of oxygen in order to increase power output from the fuel cell stack. The compressor also ensures adequate mass flow through to the cathode of the fuel cell stack.
- A heat exchanger is needed to condition the temperature of the flow. Typically, the compression in the previous step raises the temperature beyond what is required, thus, the heat exchanger must cool the flow.
- A humidifier is needed to keep the polymer membrane saturated with water. Water is a key element to proton conduction and plays a part in the efficiency of the cell. A dried out membrane is also prone to cracking which will greatly diminish the efficiency of the fuel cell due to the reactants leaking across the opposite electrodes [33].

For this study, a physics based performance model was developed in MATLAB as shown in Fig. 8. The anode side of the system is unaffected by ambient air, and has been excluded from modeling efforts. The various components on the cathode side are modeled based on simple physics and are calibrated to the current state of the art. This model can predict the power output of the fuel cell by quantifying the temperature, pressure and humidity of the flow as it passes through the components.

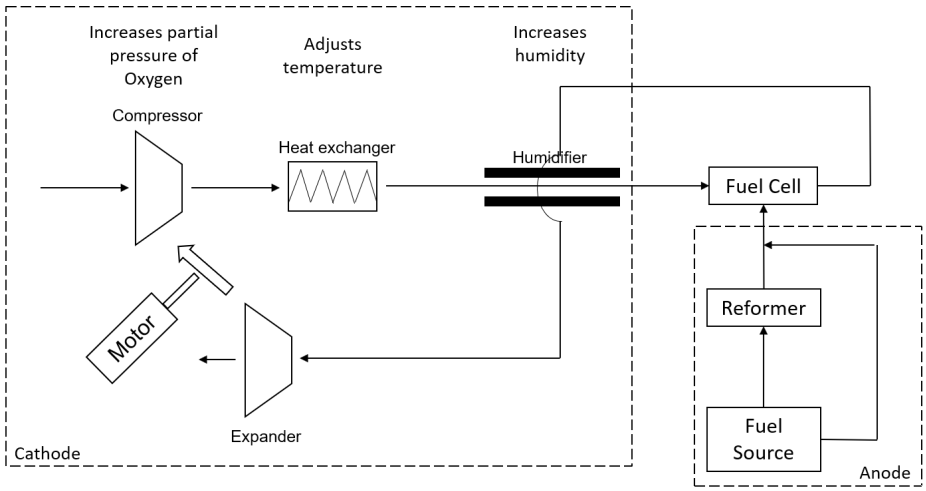


Fig. 7 Schematic of a generic fuel cell system for aviation use

The compressor is modeled as a two stage supercharger, with identical stages. The isentropic efficiency of the two stages was assumed to be 0.75 and the pressure ratio for each stage is calculated from the total pressure ratio which is the desired nominal output pressure divided by the ambient pressure. A more detailed model could include compressor maps but a constant point assumption is considered adequate for this simple case study. The desired back pressure at nominal operating conditions is assumed to be 30 psi. The output temperature, relative humidity and work required are calculated using simple isentropic and thermodynamic relations. The power required to run the compressor is provided by an electric motor which is powered through the fuel cell itself. Next, the heat exchanger is modeled as a heat transfer unit. The required heat removal (or addition) is calculated by assuming a target temperature of 80°C. Finally, the humidifier increases the humidity of the air to about 60% which is ideal for the fuel cell membrane [34].

For this study the focus is on modeling the effects of compressor performance degradation on the power output of the propulsion system. This is achieved through two parameters, the first being the mass flow rate of air through the system. The second is a scale factor related to the drop in the compressor's ability to increase the pressure of the output flow. Both of these parameters are added to the model and directly affect the performance of the system. The effect on system performance is captured by the ratio of the power output at current operating condition, which includes compressor performance degradation over the nominal system performance. Note that the nominal system performance is not a constant value, but changes with ambient altitude and weather.

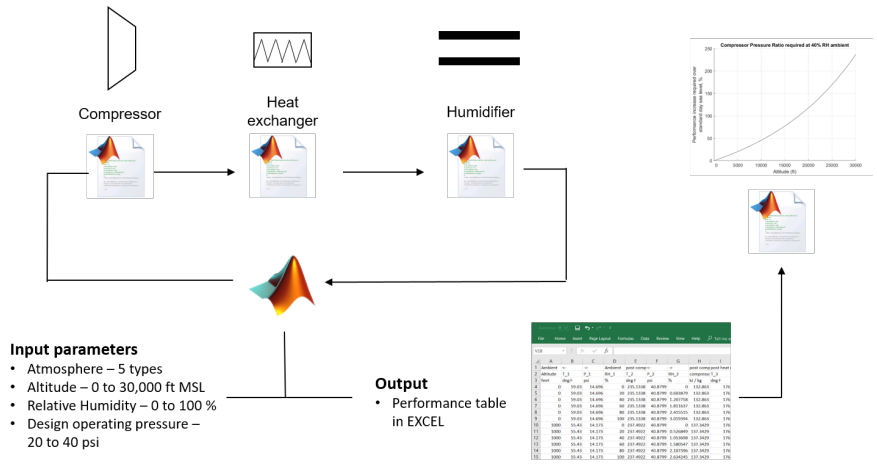


Fig. 8 Schematic of a first-principles performance model of the fuel cell system under consideration

A. Using C-FHA to Establish Hazard Severity and Component Requirements

The present case study will demonstrate the Bayesian safety assessment methodology explained in Sec. II for a hypothetical reference aircraft with performance parameters identical to those reported for the X-57-F by Borer et al. [35]. The X-57-F is a fuel cell powered variant of the X-57 Mod II distributed electric aircraft concept being designed by NASA for the Scalable Convergent Electric Propulsion Technology Operations Research (SCEPTOR) program. Since the purpose of this case study is to merely demonstrate the proposed safety assessment method, the performance model of Borer et al. [35] is assumed valid, although the X-57-F is slated to utilize a Solid Oxide Fuel Cell (SOFC) as against a PEM fuel cell considered for this case study. The present case study will consider the Take-off Field Length (TOFL) as a safety critical parameter of interest under power degradation scenarios.

1. Reference Aircraft Sizing and Performance

Sizing and performance of the reference aircraft is based on the X-57-F as mentioned above and includes information available during the early design phase. The drag polar published by Borer et al. [35] is fitted with a quadratic polynomial in the lift coefficient to give,

$$C_D = 0.0282 + 0.0483 \cdot C_L^2 \tag{6}$$

Additional parameters of interest for the hypothetical aircraft (same as X-57-F) are given in Table 2.

2. Take-Off Analysis

For the take-off phase of flight, TOFL required is considered as the safety metric of interest under a loss of power scenario to determine hazard severity. The derivation of TOFL in the event of a continuous power degradation scenario is inspired by the work of Armstrong [14], and given in Appendix A. Eq. 29 in conjunction with Eq. 24, 30 – 32 can be used to compute the TOFL required for the reference aircraft under a given failure scenario. If this TOFL required is greater than the TOFL available at the airport, the hazard severity can be considered to be catastrophic. Figure 9 shows the variation of TOFL required with a continuous loss of power and a range of TOFL available on a hot day for a airports located at an altitude of 9000 feet above mean sea level. The high altitude hot day condition is chosen as one of the most critical take-off conditions that the reference aircraft may have to face. The red areas show where TOFL required is greater than TOFL available, suggesting the presence of a catastrophic hazard in those conditions. Blue areas suggest areas where sufficient runway may be available to either abort or continue take-off procedure to reach V_{TO} after a failure causing partial loss of power. Yellow areas suggest the TOFL required is almost equal to TOFL available, suggesting decision makers to remain cautious while assigning hazard severity to these cases.

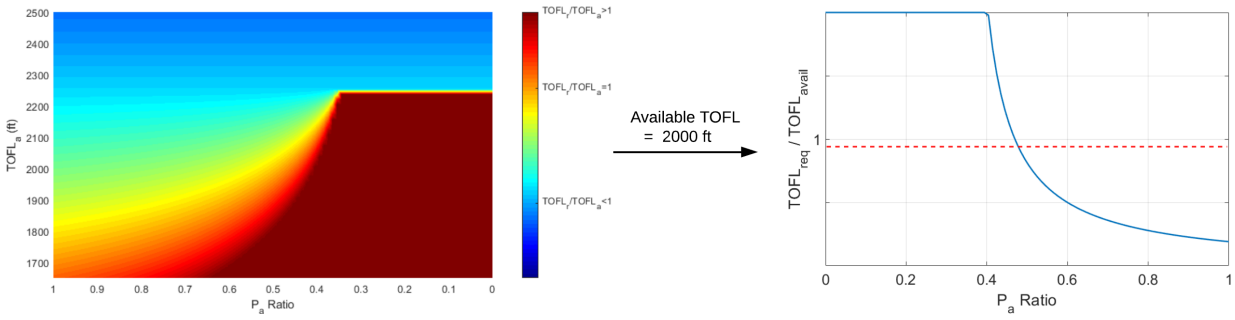


Fig. 9 Required TOFL as a function of TOFL available and Power available after failure

For the case study of interest, TOFL available is fixed at 2000 feet. While this would be considered inadequate for most commercial airports, it is not an unreasonable assumption for a general aviation aircraft. The corresponding TOFL required to available ratio is also shown by Fig. 9, with the red line providing a conservative estimate regarding when to consider the hazard catastrophic to account for uncertainty in model parameters.

3. Allocating Reliability Requirements at the Component Level

The next step in the C-FHA process is to determine the effect of component failure or degradation on the system level function of interest. For this case study, a degradation in the compressor's performance and battery failure

Parameter	Value
MTOW	1364 kg
Take-off P_{req}	145.2 kW
$C_{L_{max}}$	1.662
η_{power}	0.92
η_{prop}	0.8
μ_B	0.5
μ_r	0.02
PEM FC Power	120 kW
Take-Off Battery Power	38 kW

Table 2 Reference aircraft: Summary of parameters of interest

will be considered by quantifying their effect on power available during take-off. In realistic scenarios, a reliability block diagram (RBD) will need to be constructed to determine the overall system reliability with respect to functional degradation scenarios. For this case study, it is sufficient to assume independent failures of the battery and the compressor since these systems are connected to the electric motors in parallel, and the probability of both failing together can be neglected.

The battery is the simpler case of the two. For the reference aircraft under consideration, the battery supplies 38 kW of power for take-off as given by table 2. Thus, battery failure means a power degradation of 24%, which means the aircraft will have only 76% power available since it is installed in parallel to the fuel cell.

In the case of a compressor, a seal / gasket failure, bearing failure, and a valve failure explain more than 80% of the failure modes observed [36]. These failure generally result in a degradation in the compressor's performance rather than a total failure. To model the degraded pressure output of the compressor, a scale factor is applied to the output flow pressure. The second parameter which is affected is the mass flow rate of air through the system to the cathode of the fuel cell stack. To obtain the critical output degradation case, the scale factor is varied from 1.0 to 0.5 in decrements of 0.1. The nominal air flow, calculated to be 0.085 kg/s, is varied in decrements of 0.005 kg/s to 0.05 kg/s. For a higher fidelity modeling, the coupling between output flow pressure and mass flow rate can be established through the use of a compressor map. The effect of the mass flow rate on the power output is easy to model. Since the quantity of reactants decreases, the power decreases by an equal ratio. The effect of the pressure on the reaction is more involved and is modeled here through the Nerst Equation for this reaction as shown in Eq. 7 [37]. Note that the Nernst equation only models the effect on the individual fuel cell voltages but not power output directly. Here, the current density output is assumed to be unchanged and thus does not affect the power output. The effect of pressure on the current density requires a high fidelity model of the stack, which is outside the scope of this paper.

$$E = E^0 - \frac{RT}{2F} \ln \frac{1}{p_{H_2} p_{O_2}^{1/2}} \tag{7}$$

The most critical case is found to be the one where the output pressure scale factor is 0.5 and the mass flow is 0.05 kg/s at an altitude of 9000 feet on a hot day (+45^{0}F). This results in a drop of fuel cell output power by about 42%. This means that the combined fuel cell + battery system can provide only 68% of the power required for take-off. Figure 10 shows the outputs of the C-FHA process applied to the compressor that supplies the fuel cell with compressed air, and the battery that is connected in parallel to the fuel cell. While the compressor performance degradation results in a hazardous condition, battery failure results in a condition somewhere between hazardous and major in severity. Since the hypothetical reference aircraft is assumed to be identical to the X-57-F, it falls under assessment level I as given in table 1. Thus, compressor degradation should have a failure rate of $< 10^{-5}$ while battery failure should have a failure rate of roughly $< 5 \times 10^{-5}$. These values will be used in the compliance findings to be made.

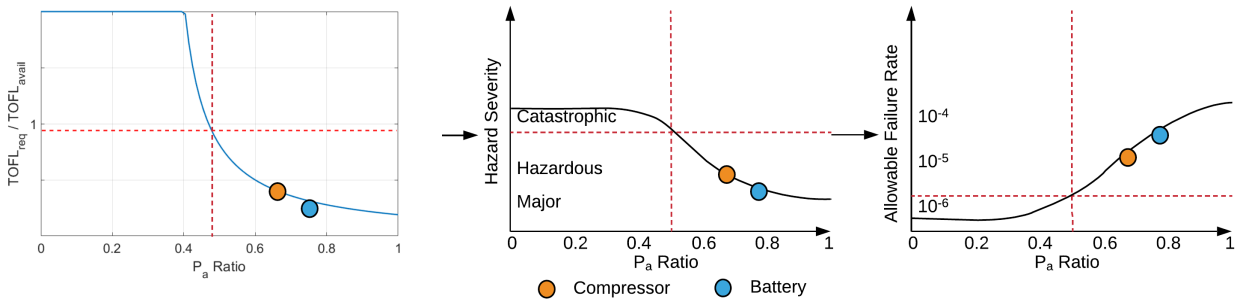


Fig. 10 C-FHA results: Component failure rate requirements

B. Evaluating Probability of Component Failures

Two analysts *A* and *B* are considered to evaluate the probability of failure of the battery and the compressor. For both components, a Poisson likelihood model is assumed since failures generally occur during operation with the number of failures and corresponding operating time being the information documented. Both analysts work off a common set of gathered data for the two components as given in Table 6 found in Appendix B. This data is gathered after both analysts decide on the prior distributions.

1. Posterior Estimation: Battery Failure

Analyst A does not have much knowledge about battery failures, and thus utilizes a Jeffrey's non-informative prior to represent the epistemic uncertainty in the failure rate so as to not bias the posterior. For a Poisson likelihood, the Jeffrey's non-informative prior is a Gamma distribution with shape parameter $\alpha_{prior} = 0.5$, and rate parameter $\beta_{prior} = 0$. While this prior is not proper (its integral over all possible values of λ is not 1), the posterior that results is proper. Generating the likelihood distributions using data given in Table 6 found in Appendix B, the posterior is given by a Gamma distribution with shape $\alpha_{posterior} = 0.5 + \Sigma y_i$, and the rate $\beta_{posterior} = 0 + \Sigma t_i$ [16].

$$Prior \quad : \quad \lambda_{prior_A} \sim Gamma(\alpha = 0.5, \beta = 0) \tag{8}$$

$$Likelihood \quad : \quad y_i|\lambda \sim Poisson(\lambda t_i, y_i) \propto \frac{(\lambda t_i)^{y_i} e^{-\lambda t_i}}{y_i!} \tag{9}$$

$$\begin{aligned} Posterior \quad &: \quad \lambda_{posterior_A}|\bar{y} \sim Gamma(\alpha = 0.5 + \Sigma y_i, \beta = 0 + \Sigma t_i) \\ &: \quad \lambda_{posterior_A}|\bar{y} \sim Gamma(\alpha = 17, \beta = 11922301) \end{aligned} \tag{10}$$

Eq. 10 gives Analyst A's posterior on the failure rate of battery. Analyst B also decides to use a Jeffry's prior for the battery, but disagrees with Analyst A's choice of utilizing data generated for non-Li-ion batteries for computing the failure rate. Analyst B finds out that Boeing 787 reported two battery safety events in about 104000 combined flight hours of battery operation (2 batteries per aircraft, 52000 flight hours) [38]. Knowing that the battery on 787 is a Li-ion battery, Analyst B decides to utilize a method that weighs the two evidence sets [16]. Analyst B decides that the probability that the heritage data applies to the new architecture is 10%, while the probability the Boeing 787's data applies is 100%. As a result, the data sets are weighted as follows:

$$Applicable\ Data = 0.9 \times (B787\ data) + 0.1 \times (B787 + Heritage\ data)$$

The resulting posterior for the battery failure rate for Analyst B is then given by Eq. 11.

$$\begin{aligned} \lambda_{posterior_B}|\bar{y} \quad &\sim \quad Gamma(\alpha = 0.5 + 0.1(16.5 + 2) + 0.9(2), \beta = 0.1(11922301 + 104000) + 0.9(104000)) \\ &\sim \quad Gamma(\alpha = 4.15, \beta = 1296230) \end{aligned} \tag{11}$$

2. Posterior Estimation: Compressor Failure

For the compressor failure rate estimation, Analyst A again assumes a Jeffrey's prior given in Eq. 8. Using a Poisson likelihood given by Eq. 9 and the data given in Table 6 found in Appendix B, Analyst A generates the following posterior for compressor failure rate,

$$\lambda_{posterior_A}|\bar{y} \sim Gamma(\alpha = 14.5, \beta = 336700) \tag{12}$$

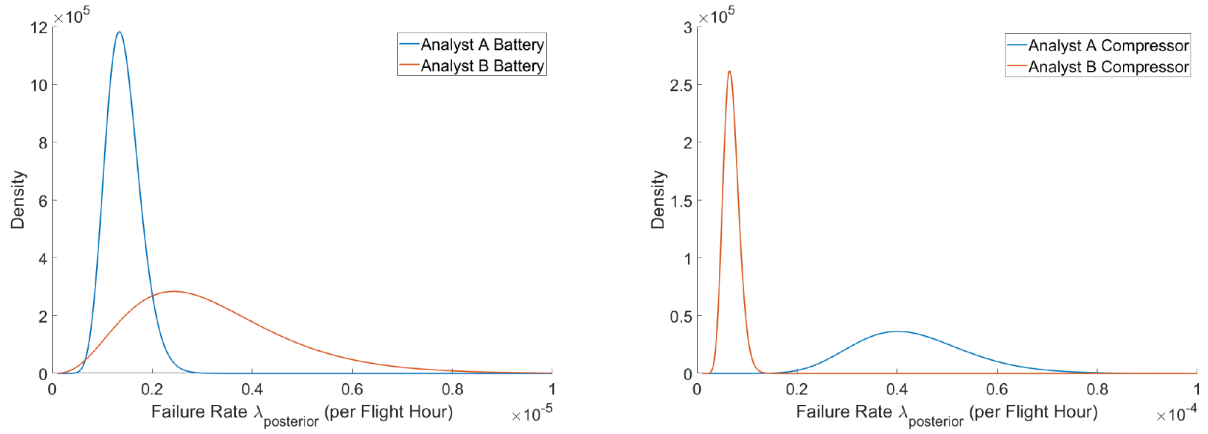


Fig. 11 Posteriors for the battery and compressor failure rate

Analyst B happens to be familiar with compressor design and knows that a typical compressor is designed to have a 5% failure rate after 25,000 hours of operation [39]. That is equivalent to having 5 failures in 100, after operating for 25,000 hours each. Thus, Analyst B's prior is given by Eq. 13

$$\lambda_{prior_B} \sim Gamma(\alpha = 5, \beta = 2.5 \cdot 10^6) \tag{13}$$

$$\lambda_{posterior_B} \sim Gamma(\alpha = 19, \beta = 2836700) \tag{14}$$

Figure 11 shows the posteriors for battery and compressor failure computed by Analyst A and Analyst B. Since Analyst B considers heritage data for battery failure less applicable compared to more recent data from the Boeing 787 with a much higher failure rate, we can see that the corresponding posterior is more spread out compared to Analyst A's posterior and suggests higher uncertainty in its true value. For the compressor, Analyst B utilizes SME knowledge on compressor failure rate to highly bias the failure rate towards the left with an informative prior. As a result, the value and spread for Analyst B's compressor failure rate is seen to be much lower compared to Analyst A. With the posterior probabilities now ready, the two analysts can proceed to make a compliance assessment.

C. Making a Compliance Assessment

With the component level reliability (allowable failure rate) requirement available from Sec. III.A.3 and failure rate posterior available from Sec. III.B, Analyst A and Analyst B can utilize the Bayesian decision framework described in Sec. II.C to make a compliance finding. The loss function agreed upon by both analysts in consultation with regulators is given in Table 3. The rational behind this loss function is as follows: (i) Finding a component to be compliant when in fact it is not can be a costly mistake and is therefore penalized the highest, (ii) Finding a component to be non-compliant when in fact it is compliant, while undesirable, is not as undesirable as the previous case, and is therefore penalized to a lesser extent, (iii) Finding a component to be (non-) compliant when it is in fact (non-) compliant is desirable, and is given a negative score to indicate a negative loss (desirable). The loss function considered here is merely an example and can be customized by decision makers as needed in order to better suit their purpose.

True State	Decision Action a	
X	$a_1 = \{Compliant\}$	$a_2 = \{Non-Compliant\}$
$X_1 = \{Compliant\}$	-2	1
$X_2 = \{Non-Compliant\}$	4	-2

Table 3 Loss function $L(X, a)$

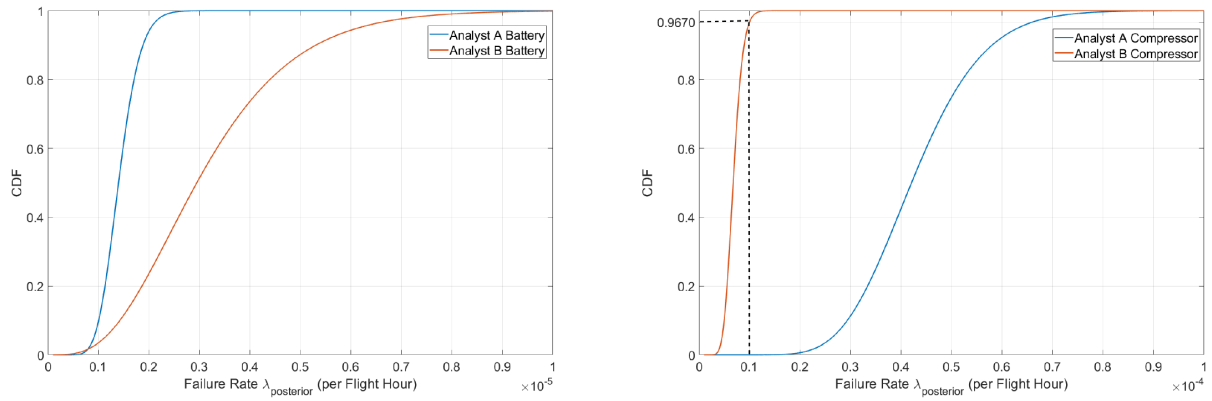


Fig. 12 Posterior CDFs to determine p_A and p_B

The Bayesian expected loss given by Eq. 3 gets simplified because of the loss function provided by Table 3 to give,

$$\rho(a_1, p_A) = L(X_1, a_1) \cdot p_A + L(X_2, a_1) \cdot (1 - p_A) \quad (15)$$

$$\rho(a_2, p_A) = L(X_1, a_2) \cdot p_A + L(X_2, a_2) \cdot (1 - p_A) \quad (16)$$

$$\rho(a_1, p_B) = L(X_1, a_1) \cdot p_B + L(X_2, a_1) \cdot (1 - p_B) \quad (17)$$

$$\rho(a_2, p_B) = L(X_2, a_1) \cdot p_B + L(X_2, a_2) \cdot (1 - p_B) \quad (18)$$

Where p_A and p_B are the probability of the component meeting its requirements computed via the posterior CDFs (see Fig. 12) of Analyst A or Analyst B respectively and are given in Table 4. As stated in Sec. II.C, the minimum of the expected loss given by equations 15-16 should inform the compliance action to be taken by Analyst A (and similarly by Analyst B).

	$p(\lambda_{posterior} < \lambda_{allowable})$	
Component	Analyst A	Analyst B
Compressor	5.786×10^{-6}	0.967
Battery	1	0.999

Table 4 Probability of meeting failure rate requirements

Table 5 gives the expected loss for the decision actions a_1, a_2 for Analyst A and Analyst B for the two components of interest.

	Analyst A		Analyst B	
Component	$\rho(a_1, p_A)$	$\rho(a_2, p_A)$	$\rho(a_1, p_B)$	$\rho(a_2, p_B)$
Compressor	4	-2	-1.802	0.901
Battery	-2	1	-1.994	0.997

Table 5 Expected loss due to available decision actions for the two analysts

The decision action that minimizes the expected loss is considered *Bayes action* and should be chosen. It is clear from table 5 that Analyst A should find the battery $a_1 = \{compliant\}$, while finding the compressor $a_2 = \{non - compliant\}$. At the same time, Analyst B should find both the battery and the compressor $a_1 = \{compliant\}$. This difference in outcomes can be attributed to the prior chosen by Analyst B for modeling the epistemic uncertainty in the compressor failure rate which biased the posterior towards lower values.

IV. Conclusions and Future Work

Existing safety assessment methods fall short when it comes to assessing failure probability and severity for novel aircraft concepts and technologies due to the lack of available data. The present work proposes a safety assessment methodology that combines Continuous Functional Hazard Assessment (C-FHA) with Bayesian probability and decision framework to supplement existing safety analysis techniques.

C-FHA utilizes available system performance models to compute safety critical metrics of interest under continuous functional degradation scenarios. The computed safety critical metrics can be analysed by decision makers to assign hazard severity to functional degradation scenarios. When system architectural and performance models allow the determination of component failure in terms of top level functional degradation, the generated hazard severity curves can be utilized to allocate failure rate requirements at the component level.

Instead of merely using data, Bayesian probability assessment utilizes information - consisting of data, models, and other available information like SME knowledge. A Bayesian probability assessment thus allows the analyst to provide a comprehensive treatment of aleatory as well as epistemic uncertainty. Finally, a Bayesian decision framework described allows analysts and decision makers to make a determination on compliance findings through a mathematically defensible framework.

The major contribution of this paper is the integration of Bayesian inference and decision methods with C-FHA to create a methodology for risk assessment that is applicable to any system under consideration. A case study was provided to help readers understand the methodology better by demonstrating it on a simplistic problem. Future work will look at combining this methodology with the aircraft preliminary sizing process to include reliability requirements and compliance considerations early in aircraft design. Additional case studies on transformational aviation concepts in GA, as well as on the More-Electric Aircraft will be considered for the future.

Appendix

A. TOFL Required under Continuous Power Degradation

The derivation of TOFL under power loss presented here is inspired by the work of Armstrong [14]. For a successful take-off, the TOFL is decomposed into (i) ground roll (s_g), (ii) rotation (s_R), and (iii) Climb for clearing obstacle (s_{obs}) [40]. In case of a critical thrust loss during take-off before the decision speed V_D, the Balance Field Length (BFL) includes the distance covered to accelerate from 0 to V_D along with the distance required to brake from V_D back to 0.

$$\begin{aligned} ds &= V_\infty dt \\ &= \frac{d(V_\infty^2)}{2(\frac{dV_\infty}{dt})} \end{aligned} \tag{19}$$

$$\begin{aligned} \frac{dV_\infty}{dt} &= \frac{1}{m}\left(T - D - \mu_r(W - L)\right) \\ &= g\left(\frac{T}{W} - \mu_r - \frac{\rho_\infty V_\infty^2}{2(\frac{W}{S})}(C_D - \mu_r C_L)\right) \end{aligned} \tag{20}$$

Substituting Eq. 19 into Eq. 20 gives,

$$s_g = \int_0^V \frac{d(V_\infty^2)}{2g(K_T + K_A V_\infty^2)} \tag{21}$$

$$K_T = \left(\frac{T}{W}\right) - \mu_r \tag{22}$$

$$K_A = \frac{-\rho_\infty}{2(\frac{W}{S})}(C_D - \mu_r C_L) \tag{23}$$

Eq. 21 gives the distance covered by the aircraft under ground roll when a thrust T acts on it. In case of a failure just before decision speed, the distance covered till V_D is given by integrating Eq. 21,

$$s_{g_1} = \frac{1}{2gK_A} ln\left(\frac{\frac{K_T}{K_A} + V_D^2}{\frac{K_T}{K_A}}\right) \tag{24}$$

where K_T is evaluated at $V = 0.7 \cdot V_{TO}$ for the present case. To compute the decision speed of the aircraft, the ground roll for the braking phase is calculated by assuming the pilot cuts the power upon failure, and applies breaks. Thus, the thrust term in Eq. 22 is set to zero, and rolling friction coefficient μ_r in Eq. 23 is replaced by the braking coefficient μ_B as given in Table 2.

$$s_{g_2} = \frac{1}{2gK_{A_D}} ln\left(\frac{\frac{K_{T_D}}{K_{A_D}}}{\frac{K_{T_D}}{K_{A_D}} + V_D^2}\right) \tag{25}$$

$$K_{T_D} = -\mu_B \tag{26}$$

$$K_{A_D} = \frac{-\rho_\infty}{2(\frac{W}{S})}(C_D - \mu_B C_L) \tag{27}$$

Eq. 25 gives the distance needed to stop and aircraft from the decision speed while reducing thrust to zero and applying breaks. The Balanced Field Length (BFL) is given as,

$$BFL = s_{g_1} + s_{g_2} \tag{28}$$

For a given runway length, the speed at which the difference between runway length and BFL is zero can be obtained through a fixed point iteration. This speed is called the decision speed V_D, reaching which an aircraft has no choice but to continue take-off procedure. Thus, the critical safety case is when a loss of thrust occurs just after the decision speed. In such cases, the TOFL is given by,

$$TOFL = s_{g_1} + s_{g_{fail}} + s_R + s_{obs} \tag{29}$$

where $s_{g_{fail}}$ is the distance covered by the aircraft to reach the take-off velocity V_{TO} from V_D under a thrust degradation scenario. Since the case study deals with a fuel cell powered propeller aircraft, power available is the quantity of interest. The rest of the terms required to compute TOFL are given as,

$$s_{g_{fail}} = \int_{V_D}^{V_{TO}} \frac{V^2\, dV}{g\left(K_A V^3 + \frac{\eta_{prop} P_{fail}}{W}\right)} \tag{30}$$

$$s_{obs} = R \cdot sin\left(cos^{-1}(1 - \frac{h_{obs}}{R})\right) \tag{31}$$

$$R = 6.96 V_{stall}^2 / g$$

$$s_R = 1 \cdot V_{TO} \tag{32}$$

where the distance required to rotate and clear the obstacle is calculated using equations provided by Anderson [40].

B. Component Failure Data

Battery		Compressor	
# Failures y_i	Operating Time t_i (hrs)	# Failures y_i	Operating Time t_i (hrs)
8.5	$5 \cdot 10^6$	0	$0.0978 \cdot 10^6$
1	1, 564, 315	1	$0.125 \cdot 10^6$
7	4, 651, 560	2	$0.0595 \cdot 10^6$
0	506, 426	11	$0.0544 \cdot 10^6$

Table 6 Component failure data obtained from databases [41, 42]

References

[1] AOPA, "Aircraft Owners and Pilots Association - What is General Aviation?" Online: https://www.aopa.org/-/media/files/aopa/home/advocacy/what_ga.pdf, Accessed May 3, 2019.

[2] FAA, "Revision of Airworthiness Standards for Normal, Utility, Acrobatic, and Commuter Category Airplanes," Federal Register, online: https://www.federalregister.gov/documents/2016/12/30/2016-30246/revision-of-airworthiness-standards-for-normal-utility-acrobatic-and-commuter-category-airplanes, 2017.

[3] ASTM, "Committee F44 on General Aviation Aircraft," online: https://www.astm.org/COMMITTEE/F44.htm, accessed May 3, 2019.

[4] FAA, "83 FR 21850 - Accepted Means of Compliance; Airworthiness Standards: Normal Category Airplanes," Federal Register, online: https://www.govinfo.gov/app/details/FR-2018-05-11/2018-09990, 2018.

[5] Bleu-Laine, M.-H., Bendarkar, M. V., Xie, J., Briceno, S., and Mavris, D. N., "A Model-Based System Engineering Approach to Normal Category Airplane Airworthiness Certification," *AIAA Aviation Forum*, Dallas, TX, 2019.

[6] "SAE ARP4761: Guidelines and Methods for conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," , 1996.

[7] Moss, T. R., *The reliability data handbook*, ASME Press, New York, 2005.

[8] "ASTM F3230-17: Standard Practice for Safety Assessment of Systems and Equipment in Small Aircraft," , 2017.

[9] Moir, I., Seabridge, A., and Jukes, M., *System Safety*, John Wiley & Sons, Incorporated, New York, 2013, book section 4, pp. 119–158. URL http://ebookcentral.proquest.com/lib/gatech/detail.action?docID=1469444.

[10] "SAE ARP4754: Guidelines for Development of Civil Aircraft and Systems," , 2010.

[11] Hasson, J., and Crotty, D., "Boeing's safety assessment processes for commercial airplane designs," *16th DASC. AIAA/IEEE Digital Avionics Systems Conference. Reflections to the Future. Proceedings*, Vol. 1, IEEE, 1997, pp. 4.4–1 – 4.4–7.

[12] Washington, A., Clothier, R. A., and Williams, B. P., "A Bayesian approach to system safety assessment and compliance assessment for Unmanned Aircraft Systems," *Journal of Air Transport Management*, Vol. 62, 2017, pp. 18 – 33. doi: 10.1016/j.jairtraman.2017.02.003.

[13] "ASTM F3061/F3061-17: Standard Practice for Systems and Equipment in Small Aircraft," , 2017.

[14] Armstrong, M., "Identification Of Emergent Off-nominal Operational Requirements During Conceptual Architecting Of The More Electric Aircraft," Ph.D. thesis, Georgia Institute of Technology, 2011.

[15] Paté-Cornell, M., "Uncertainties in risk analysis: Six levels of treatment," *Reliability Engineering System Safety*, Vol. 54, No. 2, 1996, pp. 95 – 111. doi:10.1016/S0951-8320(96)00067-1, treatment of Aleatory and Epistemic Uncertainty.

[16] Dezfuli, H., Kelly, D., Smith, C., Vedros, K., and Galyean, W., "Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis," Tech. Rep. NASA/SP-2009-569, National Aeronautics and Space Administration, 2009.

[17] Ericson, C. A., *Hazard Analysis Techniques for System Safety*, Wiley-Interscience, Hoboken, N.J., 2005.

[18] Saglimbene, M. S., "Reliability analysis techniques: How they relate to aircraft certification," *Annual Reliability and Maintainability Symposium*, IEEE, 2009, pp. 218–222.

[19] Caldwell, R. E., and Merdgen, D. B., "Zonal analysis: the final step in system safety assessment (of aircraft)," *Annual Reliability and Maintainability Symposium*, IEEE, 1991, pp. 277–279.

[20] Armstrong, M., Garcia, E., and Mavris, D., "Aircraft Mission And System Failure Considerations For Functional Induction Based Conceptual Architecture Design," 27th International Congress of Aeronautical Sciences, Nice, France, 2010.

[21] Puranik, T., Jimenez, H., and Mavris, D., "Energy-based metrics for safety analysis of general aviation operations," *Journal of Aircraft*, Vol. 54, No. 6, 2017, pp. 2285–2297.

[22] Puranik, T. G., "A Methodology for Quantitative Data-driven Safety Assessment for General Aviation," Ph.D. thesis, Georgia Institute of Technology, 2018.

[23] An, D., Choi, J., and Won, J., "Integrated Bayesian reliability analysis under input variable and metamodel uncertainties," *51st AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference 18th AIAA/ASME/AHS Adaptive Structures Conference 12th*, 2010, p. 2594.

[24] Banghart, M., Bian, L., Strawderman, L., and Babski-Reeves, K., "Risk assessment on the EA-6B aircraft utilizing Bayesian networks," *Quality Engineering*, Vol. 29, No. 3, 2017, pp. 499–511. doi:10.1080/08982112.2017.1319957.

[25] Bonis, A., *Bayesian Reliability Demonstration Plans*, 1966. doi:10.2514/6.1966-25112.

[26] Youn, B., and Wang, P., *Bayesian Reliability Based Design Optimization under Both Aleatory and Epistemic Uncertainties*, 2006. doi:10.2514/6.2006-6928.

[27] "Reactor safety study. An assessment of accident risks in US commercial nuclear power plants. Executive summary," Tech. rep., United States Nuclear Regulatory Commission, 1975.

[28] Guarro, S., "Risk assessment of new space launch and supply vehicles," *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012*, 2012, pp. 5157–5164.

[29] Guikema, S. D., and Paté-Cornell, M. E., "Bayesian analysis of launch vehicle success rates," *Journal of spacecraft and rockets*, Vol. 41, No. 1, 2004, pp. 93–102.

[30] Kelly, D. L., "Risk Analysis of the Space Shuttle: Pre-Challenger Bayeisan Prediction of Failure," Tech. rep., Idaho National Laboratory (INL), 2008.

[31] Lee, P. M., *Bayesian statistics an introduction*, 4th ed., Chichester, West Sussex ; Hoboken, N.J., 2012.

[32] R.Dervisoglu, "Diagram of a proton conducting solid oxide fuel cell," `https://upload.wikimedia.org/wikipedia/commons/9/90/Solid_oxide_fuel_cell_protonic.svg`, 2012. [Online; accessed 29-October-2018].

[33] Larminie, J., *Fuel Cell Systems Explained*, John Wiley and Sons, 2003.

[34] Lee, P. H., and Soon Hwang, S., "Performance Characteristics of a PEM Fuel Cell with Parallel Flow Channels at Different Cathode Relative Humidity Levels," *Sensors (Basel, Switzerland)*, Vol. 9, 2009, pp. 9104–21. doi:10.3390/s91109104.

[35] Borer, N., Geuther, S. C., Litherland, B., and Kohlman, L. W., "Design and Performance of a Hybrid-Electric Fuel Cell Flight Demonstration Concept," 2018 Aviation Technology, Integration, and Operations Conference, AIAA AVIATION Forum, Atlanta, 2018. doi:10.2514/6.2018-3357.

[36] Chandler, G., Denson, W. K., Rossi, M. J., and Wanner, R., "Failure mode/mechanism distributions," Report, RELIABILITY ANALYSIS CENTER GRIFFISS AFB NY, Sept 1991. URL `https://apps.dtic.mil/docs/citations/ADA259655`.

[37] O'Hayre, R., Cha, S., Colella, W., and Prinz, F. B., *Fuel Cell Fundamentals*, John Wiley Sons, 2016.

[38] Board, N. T. S., "Auxiliary Power Unit Battery Fire Japan Airlines Boeing 787-8, JA829J," Incident Report NTSB/AIR-14/01, National Transportation Safety Board, Jan 7, 2013 2013. URL `https://www.ntsb.gov/investigations/pages/boeing_787.aspx`.

[39] Zaretsky, E., Hendricks, R. C., and Soditus, S., "Weibull-based design methodology for rotating aircraft engine structures," Report NASA/TM-2002-211348, NAS 1.15:211348, E-13091, NASA, June 2002.

[40] Anderson, J. D., *Aircraft performance and design*, McGraw Hill Education (India), 2010.

[41] Denson, W., Chandler, G., Crowell, W., and Wanner, R., *Nonelectronic parts reliability data*, Reliability Analysis Center, New York, 1991.

[42] "Survey of Ranges of Component Reliability Data for use in Probabilistic Safety Assessment," Technical document, IAEA, June 1989. URL `https://www-pub.iaea.org/MTCD/Publications/PDF/te_508_web.pdf`.